International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Enhancing Image Security Using DNA and Deep Steganography

Mafnitha K K
Assistant Professor
Dept. of Computer Science Engineering(Cyber Security)
Vimal Jyothi Engineering College
Email: mafnitha@vjec.ac.in

Anju K B
Assistant Professor
Computer Science and Engineering Department
Government Engineering College Wayanad
Email: anjukb@gecwyd.ac.in

***Abstract*—This project is aimed at providing a secure way of sending confidential images between users. Application is built to provide protection of the sensitive image being transmitted. Modern advancements have made it incredibly convenient to both send and store digital images online. Images often contain sensitive personal information, such as photographs, identification documents, medical records etc. Unauthorized access to these images can lead to identity theft, privacy invasion, and personal harm. Image security is crucial for several reasons, spanning personal privacy, corporate confidentiality, intellectual property protection and national secu rity. In order to solve the above described problems, this project provide a novel encryption method for color pictures that utilizes convolutional autoencoder, DNA and steganography. Convolutional autoencoders can compress image data into a lower dimensional latent space before encryption. Image encryption scheme using DNA along with multiple chaotic sequences and substitution boxes provide security of the image. Hiding images within other images involves a technique known as steganography. In this process a secret image is embedded within a cover image making it imperceptible to the human eye. The security of the proposed method has been evaluated using several parameters, such as histogram of the cipher image, entropy, NPCR, UACI etc. The result shows that it a compelling approach to secure images against various attacks.**

***Keywords*– Convolutional neural network, autoencoder, chaos, DNA coding, deep learning, colour image encryption, steganography.**

I. INTRODUCTION

The internet has grown in popularity as a means of transferring digital media between people, businesses, organizations, governments, miltary etc. Information security has gained global attention as a result of the Internet's data explosion. The need for secure communication and data protection has become paramount. Although information hiding techniques have been around for a while, their significance has lately increased due to a rise in data traffic via social media and the internet. The most widely used technique for protecting information is cryptography, however steganography has become more well known recently. The technique of hiding a message by enclosing it in another safe media is known as steganography.

1) Convolutional Neural Networks : Convolutional Neural Networks (CNNs) are specialized neural networks designed to process and interpret two-dimensional data, making them particularly well suited for image and video analysis. Convolutional layers enable CnN to automatically extract characteristics from images, which makes them ideal for applications like object detection, facial recognition, and image categorization [1]. It is an extended version of artificial neural network(ANN) which is mainly used to extract the feature from the grid like matrix dataset [2] [3]. An example illustration of a CNN can be seen in Figure (1)

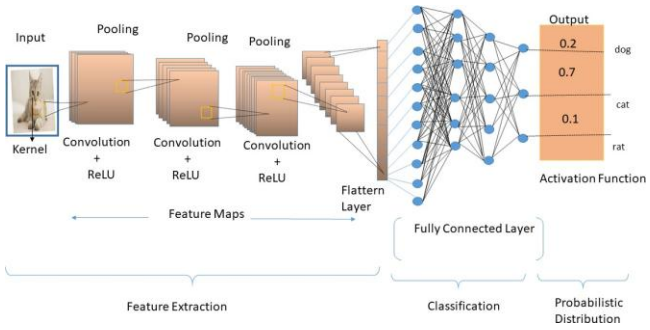

Fig. 1. Convolution neural network

2) DNA Encryption: DNA encryption is a cutting-edge field that merges computer science and molecular biology to enhance data security. By converting image pixels into DNA molecules for encryption, DNA based cryptographic methods offer high security [4]. The use of DNA computing in cryptography provides exceptional parallelism, energy efficiency and storage capacity, making it a promising technology for secure communications [5]. Researchers have proposed various encryption techniques, such as chaotic diffusion operations and cryptographic key generation, to develop robust DNA encryption algorithms that resist attacks and ensure data confidentiality.

3) Steganography: In order to provide secure communication, steganography is the technique of hiding information under cover objects to avoid discovery. It involves hiding messages in ways that make the presence of a hidden message undetectable to unintended recipients [6]. By utilizing various techniques such as altering the least significant bits of data

in images, text, and audio files to embed secret information while maintaining the original appearance. Steganography has evolved to include methods like masking, filtering, encryption, and scattering to enhance security against detection and steganalysis attacks, allowing for the concealment of unlimited text sizes within different types of media [7].

II. Related works

The most widely used image steganography technique for quickly and efficiently hiding secret data in images is the least significant bit (LSB) replacement method. Secret data is hidden using modified LSB substitution method and uses edge preserving modules to ensure minimal distortion. Robustness is not a component of this proposed method. More LSB are used for edges than smooth areas to provide imperceptibility [8]. Rahman et al.'s [9] LSB substitution method offers a significant improvement over traditional techniques by optimizing embedding strategies and incorporating enhanced security measures. The technique represents a valuable advancement in the field of digital image steganography, balancing the need for high embedding capacity, imperceptibility, and robustness against detection. This technique employs a more sophisticated method for selecting pixels and bits to modify, reducing the chance of detectable patterns. This could involve randomized bit substitution or adaptive algorithms that consider the image content.

A variety of papers have presented an image encryption scheme based on a mixture of chaotic systems, providing detailed description of the algorithm and security analysis. An encryption scheme based on a one dimensional logistic map combined with a random key search crite rion for high security image encryption has been proposed [10]. In order to demonstrate the high level of protection against various attacks, a novel image encryption system using DNA sequence operations and chaos systems was presented in [11]. In symmetric key image encryption and decryption, 3D chaotic logistic maps with DNA encoding have been used for image pixel confusion and diffusion. A cryptosystem that integrates bit level diffusion with DNAcoding for medical image encryption was introduced by [12]. This dual-layered approach aims to offer robust security by combining spatial and biological encryption principles. The cryptosystem's scalability for large-scale medical imaging datasets needs further exploration, especially considering the increasing size and complexity of medical data [13].

In recent years, there has been a lot of research work on the use of deep learning achieve image steganography. One such method is [14] the encoding and decoding neural networks are com posed of two almost identical neural networks . It will help the network to model very detailed features of images in their temporal spaces. The cover and the hide images are combined in a channel, but only an embedded image is shown to the network throughout the embed process. Exponential linear unit(ELU) and batch normalization are chosen to achieve better results and faster convergence []. The integration of autoencoders and compressive sensing in the form of joint compressive autoencoders presents a novel and efficient approach to hiding multiple images within a single image [15]. This method leverages the strengths of both deep learning and signal processing to achieve high-capacity, high quality image embedding. Inspite of the good capacity StegNet provides there's still some noise generated at non textured areas in the generated images.

A method was introduced a filtering based hybrid approach using LSB image steganography and AES cryptography. The [16] proposed method focuses on bitmap images for LSB steganography, limiting the application to only this specific image format. By combining elliptic curve cryptography and deep neural networks, an efficient image steganography method has been introduced [17]. In order to enhance its antidetection capabilities, the secret image is changed using the discrete cosine transform and the elliptic curve cryptography, which are then used to encrypt the altered image [18].

III. PROPOSED METHODOLOGY

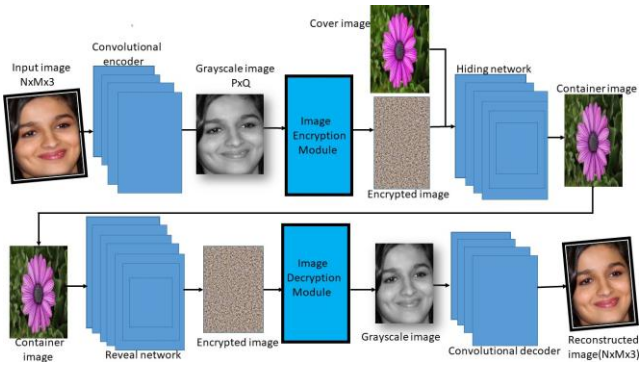

Fig. 2. Architecture

The proposed system is composed of three sections which is shown in Figure 3.1. This system combines convolutional autoencoding, DNA encryption, and image steganography to create a secure and efficient method for image encryption and decryption. The use of neural networks ensures the extraction and reconstruction of high-quality image features, while DNA encryption provides robust security. Steganography adds an additional layer of concealment, making it difficult for unauthorized users to detect the presence of encrypted information. This multi-faceted approach enhances the overall security and privacy of image data.

A convolutional autoencoder is a neural network used for unsupervised learning of efficient codings. Convolutional autoencoder(CAE) consists of two main parts: the encoder and the Convolutional autoencoder(CAE) consists of two main parts: the encoder and the decoder.Autoencoders will reduce the dimension of the orginal image to reduce the complexity of encoding process. By learning a compact representation of the input data, they can reduce the number of features while preserving essential information.In image compression, autoencoders can encode high resolution images into a lower-dimensional representation and then decode them

back to recover the image.

The next step is developing an autoencoder model. The model architecture comprises an encoder and a decoder. The encoder takes an input image and processes it through convolutional layers. The layer consist of Conv2D layer that applies a 3x3 kernel with 32 filters followed with a ReLU activation. Following the convolutional layer, a MaxPooling2D layer with a 2x2 window and same padding reduces the spatial dimensions by selecting the maximum value within each 2x2 region. This downsampling step helps to create a compact representation. A second MaxPooling2D layer downsamples the feature maps again, resulting in an even smaller representation. The final output of the encoder is the encoded representation, which has a shape of 16x16x16. This condensed representation captures essential information from the orginal image.

The decoder will reconstruct the original input image from the encoded representation. It starts with a Conv2D layer (16 filters, 3x3 kernel, ReLU activation, same padding) to expand the feature maps. An UpSampling2D layer with a 2x2 window increases the spatial dimensions by repeating the values within each 2x2 region. This step upsamples the feature maps. Another Conv2D layer with 32 filters, 3x3 kernel, ReLU activation, same padding further refines the features. A second UpSampling2D layer expands the feature maps again, restoring the spatial dimensions. The final layer is a Conv2D layer with a single filter and sigmoid activation. This layer produces the reconstructed image, aiming to match the original input image.

In order to provide a high level of security, the encryption method is combined with chaos and DNA.

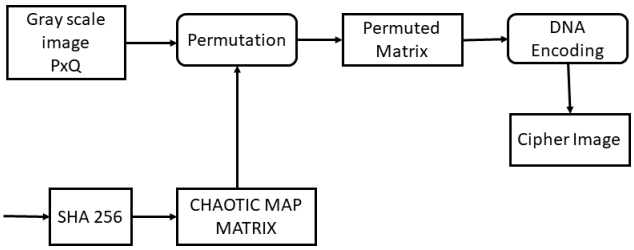

Fig. 3. Flow of the Encryption method

1) Generating a Chaotic Map Matrix
The first step is to generate a chaotic map matrix from an input matrix. By Flattening the input matrix and converted into byte string. The byte string is hashed using the SHA-256 algorithm. In order to match the size of the input matrix and to adjust the original matrix dimensions, the hashed value must be repeated. This forms the chaotic map matrix, which contains pseudo-random values based on the input matrix.

2) Permuting the Original Matrix
Using the chaotic map matrix, the original matrix is permuted. Row and column indices are sorted based on the values in the chaotic map matrix. The original matrix is permuted first by rows and then by columns using the sorted indices. The result is a permuted matrix and the indices used for permutation.

3) Encoding the Matrix to DNA Sequences
Each element in the matrix is converted to a binary string representing its integer and fractional parts. The binary string is converted to a DNA sequence where
- '0' is encoded as 'AT'
- '1' is encoded as 'CG'
- '.' (for fractional parts) is encoded as 'GC'

Each row in the matrix is processed to create a corresponding row of DNA sequences, resulting in a matrix of DNA-encoded values. The ability to decode the encryption process back to the original numerical values ensures that the process is reversible, making it suitable for secure data storage and transmission.

The technique of hiding a secret image inside another image so that its presence is obscured from view is known as image steganography. The chosen image is loaded and converted to RGB format using the Python Imaging Library (PIL). The image data is processed pixel by pixel. For each pixel, the RGB color values are modified to embed the binary message. The least significant bit (LSB) of each color component (red, green, blue) in the pixel is replaced with a bit from the binary message. This is done by
- Clearing the LSB of the color component using a bitwise AND operation.
- Setting the LSB to the corresponding bit from the binary message using a bitwise OR operation.

The modified image data, which now contains the hidden message, is saved as a new image file. This file visually appears identical to the original image but contains the embedded message within its pixel data.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Loading and preprocessing images from a FaceData dataset is taken as the input. The images are resized to a target size, typically 64x64 pixels, and their pixel values are normalized to the range [0, 1]. Then the dataset is split into training and testing sets, 80-20 split to ensure the model can be evaluated on unseen data.

For this experiment the model proposed was built based on the code written in Python. The implementation model make use of deep learning environment using TensorFlow and Keras library. In this experiment, other libraries like NumPy for numerical computations, Scipy image to gather image metrics, OpenCV for image processing, PIL (Python Imaging Library) for image manipulation, Matplotlib plotting and visualization inside

the Jupyter Notebook.
The original image shown in Figure 4 is encoded using CAE .

Fig. 4. Orginal image

DNA Encryption is done to produce cipher image which is shown in (5) Then for steganising this encrypted

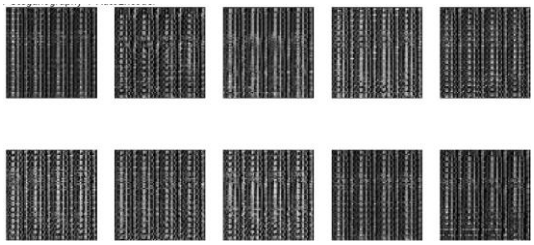

Fig. 5. Cipher image of DNA encryption

image, I have used the cover image.
At the receiver side the reverse process happens to recover the confidential data from the received image.

Fig. 6. Reconstructed image

V. Performance Evaluation

A. Model- Loss

The provided plot shows the training and validation loss of a machine learning model over 100 epochs. The model appears to have been trained effectively, with both training and validation losses decreasing and stabilizing at similar values. The similarity in the training and validation loss curves suggests good generalization to the validation set.

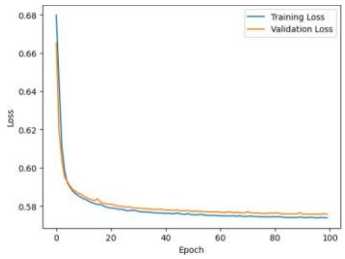

Fig. 7. Autoencoder Training Loss Graph

B. Entropy

Figure(8) represents that the entropy values of encoded and decrypted images are very close to each other for all the images. The close match between the entropy values of encoded and decrypted images indicates that the method used for embedding and extracting information is robust. The hidden data can be retrieved without significantly affecting the image's properties.

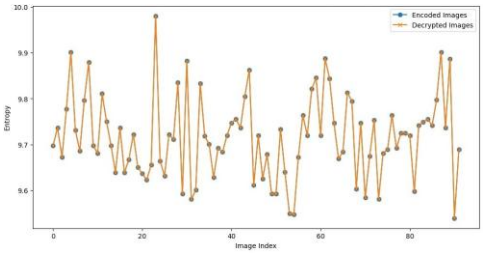

Fig. 8. Entropy comprison between Encoded and Decrypted Images

C. Histogram Analysis

The similarity in the histograms of mean pixel values for original and decrypted images in Figure(9) demonstrates that the steganographic method effectively preserves the original image quality.

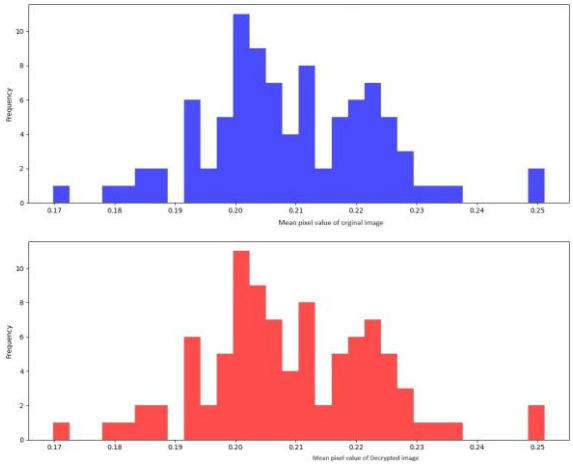

Fig. 9. Visualization of Reconstructed images

D. Security Analysis

	Ref. [19]	Ref. [20]	Ref. [15]	Our Method
Entropy analysis	7.902	7.91	7.92	7.953
Correlation analysis	0.0029	0.0012	0.0052	0.0019
Differential analysis (NPCR)	99.61%	-	99.67%	99.63%
Differential analysis (UACI)	33.46%	-	33.68%	32.38%

From the evaluation of the system it can be concluded that the entropy value is approximated to 8. Correlation analysis shows how similar the reconstructed images are to the original images. The NPCR and UACI values shows that the strongly resist differential attack. By applying multi-layer protection, the system becomes less vulnerable to cyberattacks.

VI. Conclusion

I have successfully developed and implemented a novel approach to enhance security of the image by integrating convolutional autoencoders with DNA cryptography and steganography techniques. The designed and trained a convolutional autoencoder to compress the images into a latent space representation. The autoencoder reconstruct the images with minimal loss. The chaotic map-based permutation and dna encryption method ensured additional security by shuffling the image data in a non-deterministic manner, making it difficult for unauthorized entities to decipher the original content. Image steganography is the method of transmitting secret image by hiding it inside the cover image. The security of the proposed method was evaluated using several parameters, such as entropy, histogram, correlation coefficient , NPCR, UACI etc. The findings highlight the importance of continually exploring innovative approaches to image security in an increasingly digital world. This work contributes to the broader field of image security and opens doors for further research and development in this domain.

References

[1] F. Kreuk, Y. Adi, B. Raj, R. Singh, and J. Keshet, "Hide and speak: Deep neural networks for speech steganography," *arXiv preprint arXiv:1902.03083*, 2019.

[2] X. Liu, Z. Ma, Z. Chen, F. Li, M. Jiang, G. Schaefer, and H. Fang, "Hiding multiple images into a single image via joint compressive autoencoders," *Pattern Recognition*, vol. 131, p. 108842, 2022.

[3] I. Kich, Y. Taouil, *et al.*, "Cnn auto-encoder network using dilated inception for image steganography," *International Journal of Fuzzy Logic and Intelligent Systems*, vol. 21, no. 4, pp. 358–368, 2021.

[4] N. H. UbaidurRahman, C. Balamurugan, and R. Mariappan, "A novel dna computing based encryption and decryption algorithm," *Procedia Computer Science*, vol. 46, pp. 463–475, 2015.

[5] T. Ajaz, H. Ashraf, and G. Alwakid, "Hybrid security scheme for a colored image using dna and chaotic map," in *2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, pp. 1–5, IEEE, 2022.

[6] N. Patel and S. Meena, "Lsb based image steganography using dynamic key cryptography," in *2016 international conference on emerging trends in communication technologies (ETCT)*, pp. 1–5, IEEE, 2016.

[7] M. Geleta, C. Punti, K. McGuinness, J. Pons, C. Canton, and X. Giro-i Nieto, "Pixinwav: Residual steganography for hiding pixels in audio," in *ICASSP 2022-2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 2485–2489, IEEE, 2022.

[8] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, "A novel magic lsb substitution method (m-lsb-sm) using multi-level encryption and achromatic component of an image," *Multimedia Tools and Applications*, vol. 75, pp. 14867–14893, 2016.

[9] S. Rahman, J. Uddin, H. U. Khan, H. Hussain, A. A. Khan, and M. Zakarya, "A novel steganography technique for digital images using the least significant bit substitution method," *IEEE Access*, vol. 10, pp. 124053–124075, 2022.

[10] O. M. Al-hazaimeh, "A novel encryption scheme for digital image-based on one dimensional logistic map," *Computer and Information Science*, vol. 7, no. 4, p. 65, 2014.

[11] X.-Y. Wang, Y.-Q. Zhang, and Y.-Y. Zhao, "A novel image encryption scheme based on 2-d logistic map and dna sequence operations," *Nonlinear Dynamics*, vol. 82, pp. 1269–1280, 2015.

[12] S. Patel, K. Bharath, and R. Kumar, "Symmetric keys image encryption and decryption using 3d chaotic maps with dna encoding technique," *Multimedia Tools and Applications*, vol. 79, no. 43, pp. 31739–31757, 2020.

[13] P. Mishra, C. Bhaya, A. K. Pal, and A. K. Singh, "A medical image cryptosystem using bit-level diffusion with dna coding," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 3, pp. 1731–1752, 2023.

[14] P. Wu, Y. Yang, and X. Li, "Image-into-image steganography using deep convolutional network," in *Advances in Multimedia Information Processing–PCM 2018: 19th Pacific-Rim Conference on Multimedia, Hefei, China, September 21-22, 2018, Proceedings, Part II 19*, pp. 792–802, Springer, 2018.

[15] X. Li, C. Zhou, and N. Xu, "A secure and efficient image encryption algorithm based on dna coding and spatiotemporal chaos.," *Int. J. Netw. Secur.*, vol. 20, no. 1, pp. 110–120, 2018.

[16] M. R. Islam, A. Siddiqa, M. P. Uddin, A. K. Mandal, and M. D. Hossain, "An efficient filtering based approach improving lsb image steganography using status bit along with aes cryptography," in *2014 International Conference on Informatics, Electronics & Vision (ICIEV)*, pp. 1–6, IEEE, 2014.

[17] X. Duan, D. Guo, N. Liu, B. Li, M. Gou, and C. Qin, "A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network," *IEEE Access*, vol. 8, pp. 25777–25788, 2020.

[18] W. A. Awadh, A. S. Alasady, and A. K. Hamoud, "Hybrid information security system via combination of compression, cryptography, and image steganography," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 6, p. 6574, 2022.

[19] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, "Novel medical image encryption scheme based on chaos and dna encoding," *IEEE access*, vol. 7, pp. 36667–36681, 2019.

[20] J. C. Dagadu, J. Li, E. O. Aboagye, and F. K. Deynu, "Medical image encryption scheme based on multiple chaos and dna coding.," *Int. J. Netw. Secur.*, vol. 21, no. 1, pp. 83–90, 2019.